UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JARVIS BRYANT JENKINS, on behalf of himself and all others similarly situated,

Plaintiff,

v.

INTERNATIONAL BUSINESS MACHINES CORPORATION and JOHNSON & JOHNSON HEALTH CARE SYSTEMS, INC.,

Defendants.

Case No. 7:23-cv-10244

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

INTRODUCTION

1. Plaintiff Jarvis Bryant Jenkins, on behalf of himself and the putative class, brings this case to seek redress for injuries suffered as a result of a recent data breach at Defendant International Business Machines ("IBM") of data belonging to at least one million Johnson & Johnson Health Care Systems, Inc. ("J&J") customers. According to a notice sent to Mr. Jenkins, the compromised data includes sensitive medical records protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including information about medications and associated conditions ("Private Health Information" or "PHI"). The compromised data, per the notice from IBM, also includes full names and contact information ("Personally Identifiable Information" or "PII").

2. Mr. Jenkins and the class members' PHI and PII is particularly valuable to cybercriminals who sell and trade this type of data on the dark web. The cat cannot be put back in the bag: Mr. Jenkins's PHI and PII, and the PHI and PII of all class members, will forever be vulnerable. Furthermore, despite learning of the data breach on August 2, 2023, J&J and IBM waited more than a month—until September 15, 2023—to notify Mr. Jenkins and the class of the breach.

3. The data breach was a direct result of J&J and IBM's failure to implement adequate and reasonable cybersecurity safeguards necessary to protect the PHI and PII of Mr. Jenkins and the class. Mr. Jenkins and the class provided their PHI and PII to J&J and IBM with the reasonable expectation that J&J and IBM would comply with their legal obligations to keep that information confidential and secure, and in compliance with federal regulations governing the storage of healthcare records.

4. If J&J and IBM had appropriately designed and implemented adequate and reasonable cybersecurity safeguards, the data breach would and could have been prevented. And if Mr. Jenkins and the class members knew that J&J and IBM had designed and implemented below industry standard cybersecurity safeguards, they never would have provided their PHI and PII to J&J and IBM, nor would they have relied on J&J and IBM to protect that information.

5. As a result of J&J and IBM's inadequate cybersecurity practices that caused and resulted in the data breach, Plaintiff and the class have suffered injuries including (a) damage to and diminution in the value of their PHI and PII, a form of property that J&J and IBM obtained from Mr. Jenkins and the class; (b) violation of Mr. Jenkins and the class's privacy of rights; (c) present and increased risk arising from the identity theft and fraud; (d) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; and (e) financial out-of-pocket costs incurred mitigating the materialized risk and imminent threat of identity theft.

PARTIES

I. PLAINTIFF

6. Plaintiff Jarvis Bryant Jenkins is and has been, at all relevant times, a resident and citizen of Jacksonville Beach, located in Duval County, Florida. On or around September 20, 2023, Mr. Jenkins received a letter captioned "Notice of Data Breach," dated September 15, 2023, via U.S. mail.

7. Mr. Jenkins provided his PHI and PII to Defendants on the condition that it be maintained as confidential and with the understanding that Defendants would employ reasonable safeguards to protect his PHI and PII. If Mr. Jenkins had known that Defendants would not

adequately protect his PHI and PII, he would not have entrusted Defendants with his PHI and PII or allowed Defendants to maintain this sensitive PHI and PII.

8. To the best of Mr. Jenkins's knowledge, Defendants still retain his PHI and PII and Mr. Jenkins remains vulnerable to future security breaches of Defendants' systems. As a result of the breach, Mr. Jenkins anticipates spending considerable time to mitigate and address the harm caused by J&J and IBM's conduct.

9. Mr. Jenkins has a continuing interest in ensuring that his PHI and PII is safeguarded from unauthorized access in the future.

II. DEFENDANT

10. Defendant IBM is a New York corporation with a principal place of business located at 1 Orchard Road Armonk, New York 10504-1722.

11. IBM is a technology company that, among other things, provides database management software.

12. IBM has over 288,000 employees, with offices around the United States, including its headquarters in New York and this judicial district.

13. Defendant J&J is a New Jersey corporation with a principal place of business located at 425 Hoes Lane Piscataway, New Jersey 08854-4103.

14. J&J is a subsidiary of Johnson and Johnson, which is also a New Jersey corporation.

15. J&J has over 150,000 employees, with offices around the United States, including in New York and this judicial district.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over IBM because the conduct alleged in this Complaint occurred in and/or emanated from the State of New York, and because IBM maintains its headquarters in New York.

18. This Court has personal jurisdiction over J&J because the conduct alleged in this Complaint occurred in and/or emanated from the State of New York, and because J&J maintains a substantial (and indeed massive) presence in the State of New York.

19. J&J maintains offices in the State of New York, has employees in the State of New York, and routinely does business in the State of New York. As such, it has sufficient minimum contacts in this state and has purposefully availed itself of the jurisdiction of the State of New York by, among other things, marketing and selling products and services, and accepting and processing payments for products and services with the State of New York.

20. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because J&J and IBM do business in this judicial district and the conduct at issue occurred in and/or emanated from this judicial district.

FACTS

I. CarePath

21. Janssen CarePath ("CarePath") is a patient support program which offers savings options and resources to patients to help them learn about, afford, and stay on their medication.[1] The program was created and run by J&J to help patients taking Janssen medications.[2]

22. CarePath offers resources to patients and their doctors to understand their insurance coverage and out-of-pocket costs for certain J&J medications.[3] It also assists patients and other stakeholders in identifying ways to pay for J&J medications.[4]

23. CarePath provides resources for include a variety of J&J prescription medications, including cancer medications such as: Akeega™ and Erleada®, which are used to treat prostate cancer; Balversa®, which is used to treat bladder cancer; Darzalex® and Darzalex *Faspro*®, which is used to treat adults with multiple myeloma; Rybrevant®, which is used to treat non-small cell lung cancer.[5] CarePath also provides support to patients taking medications such as: Edurant®, Intelence®, Prezcobix®, and Prezista®, which are prescribed to people living with HIV[6] and Invega®, Invega Hafyera™, Invega Sustenna®, Invega Trinza®, Risperdal®, Risperdal Consta®, which are prescribed to people with schizophrenia. Patients prescribed a number of other medications are also supported through CarePath.

24. The fact that patients, including Mr. Jenkins and class members, are prescribed these medications and may have one of the associated conditions is deeply private and personal information, which patients only entrusted to J&J on the condition that it would remain confidential.

---

[1] https://www.myjanssencarepath.com/s/helpfaq (last accessed November 21, 2023).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] https://www.janssencarepath.com/patient/important-safety-information (last accessed November 21, 2023).
[6] *Id.*

25. In 2018, J&J reported in its U.S. Transparency Report that approximately 550,000 patients were helped through CarePath.[7] By 2022, that number had risen to more than 1.16 million patients.[8]

II. IBM has an extensive history researching and preventing data breaches and was aware of the risks of a healthcare data breach.

26. For 17 years, IBM has sponsored, analyzed, and published independent research into the impact of data breaches as well as factors that can increase or mitigate the costs of these breaches.[9] Its most recent report from 2022 quantified the risk from different kinds of breaches, such as ransomware attacks, destructive attacks, supply chain attacks, human error, IT failures, and other kinds of attacks.[10] The 2022 version provided recommendations for successful security approaches as well.[11]

27. IBM also publishes reports regarding data breaches that its own cybersecurity team, X-Force, responds to.[12] IBM's 2023 "X-Force Threat Intelligence Index" report lists healthcare as representing a 5.8% share of X-Force incident response cases in 2022.[13] IBM's report notes that the proportion of healthcare cases that X-Force responded to has remained at approximately 5%-6% for the last three years.[14] Per IBM, methods used to cyberattack healthcare targets in recent years include backdoor attacks (27% of cases) and web shells (18%).[15] Adware, BEC, cryptominers, loaders, reconnaissance and scanning tools, and remote

[7] https://www.jnj.com/latest-news/2018-janssen-us-transparency-report-top-5-things-you-need-to-know (last accessed November 21, 2023).
[8] https://transparencyreport.janssen.com/_document/2022-janssen-transparency-report-pdf?id=00000188-267e-d95e-abca-7e7e58750000 (last accessed November 21, 2023).
[9] https://www.ibm.com/downloads/cas/3R8N1DZJ (last accessed November 21, 2023).
[10] *Id.* at p. 36.
[11] *Id.* at pp. 47-48
[12] *See, e.g.,* https://www.ibm.com/downloads/cas/DB4GL8YM (last accessed November 21, 2023).
[13] *Id.* at p. 49.
[14] *Id.*
[15] *Id.*

access tools comprised 9% each of all healthcare cyberattacks logged by IBM's X-Force in recent years. Data theft and digital currency mining were each identified in 25% of cases.[16]

28. Former IBM Chairman, President and CEO Ginni Rometty stated while helming the company at the 2015 IBM Security Summit, "cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world." Current Chairman and CEO Arvind Krishna opened IBM's 2022 Annual Report by recognizing the "ever-evolving cybersecurity threat landscape."

29. IBM not only recognizes the threats of cybercrime and cyberattacks but profits off them. In 2014, IBM was the fastest growing security software vendor in the world, according to IT research firm Gartner.

30. IBM itself is no stranger to data breaches as of late. It recently experienced a massive breach of its business stemming from its support of a healthcare system. In June 2023, IBM disclosed to the public that its systems were exposed to a serious vulnerability related to MOVEit Transfer.

31. The MOVEit breach involved work IBM did as a third-party vendor for the Colorado Department of Health Care Policy and Financing, which oversees Colorado's Medicaid program, Child Health Plan Plus program, and other state healthcare programs. IBM utilized an application called MOVEit Transfer to move data files in the normal course of business. This application was exploited by an unauthorized actor on or about May 28, 2023. The resulting breach exposed protected health information and personal identifying information of four million individuals.

[16] *Id.*

32. J&J utilized IBM as a service provider to manage the CarePath application and the third-party database that supports it during the data breach that occurred on August 2, 2023.[17]

33. On information and belief, since the August 2, 2023 data breach, J&J has continued to utilize IBM to manage CarePath and the third-party database containing Mr. Jenkins and Class Members' PHI and PII.

III. Data Breaches in Healthcare Have Been Increasing

34. The healthcare industry has experienced many high-profile cyberattacks in the last several years preceding this complaint's filing. Cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[18] According to the HIPAA Journal, the largest healthcare data breaches were reported in April 2021.[19]

35. For example, Broward Health experienced a cyberattack on October 15, 2021, similar to the attack on Defendants. The hackers gained access to Broward Health's system through a third party provider. As a result of this attack, Broward Health disclosed that personal identifying information, including health-related data protected by HIPAA, of 1.35 million individuals was at risk of exposure.[20] Similarly, in 2021, Scripps Health suffered a cyberattack, which effectively shut down critical healthcare services for a month and left numerous patients unable to speak to their physicians or access vital medical and prescription records.[21] University of San Diego Health suffered a similar attack a few months later.[22]

---

[17] https://www.janssencarepath.com/notice-of-data-incident (last accessed November 21, 2023).
[18] https://www.hipaajournal.com/2020-healthcare-data-breach-report/ (last accessed November 21, 2023).
[19] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed November 21, 2023).
[20]. https://apnews.com/article/technology-health-hacking-us-department-of-justice-ac59138547d6c3ca718c6ff002034686 (Last accessed November 21, 2023).
[21] https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to- internal-systems-hit-by-cyberattack-2/2619540/ (last accessed November 21, 2023).
[22] https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some- employee-email-accounts-impacted/2670302/ (last accessed November 21, 2023).

36. As of October 17, 2023, the U.S. Department of Health and Human Services' Office of Civil Rights' Breach Portal shows that 524 major health data breaches affecting 88.7 million individuals have been reported so far in 2023. Of these, about 40% have involved business associates that handle PII and HIPAA-protected data, like IBM.[23]

37. According to a report by cybersecurity firm Critical Insight, "breaches associated with third-party business associates have 'steadily risen' from 10% in the beginning of 2019 to 21% in the most recent six-month period."[24]

38. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[25]

39. Patient records, like those stolen from Defendants, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail."[26] The record sets are then sold on dark web sites to other criminals, which "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[27]

40. Data breaches in healthcare such as the one experienced by J&J and IBM have become so notorious that the Federal Bureau of Investigation ("FBI") and the U.S. Cybersecurity

[23] https://www.bankinfosecurity.com/ibm-says-631k-affected-in-johnson-johnson-database-breach-a-23335 (last accessed November 21, 2023).
[24] https://www.fiercehealthcare.com/health-tech/fewer-larger-healthcare-data-breaches-reported-h1-2023-hackers-often-targeting-third (last accessed November 21, 2023).
[25] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last accessed November 21, 2023).
[26] *Id.*
[27] *Id.*

& Infrastructure Security Agency ("CISA") have issued a warning to potential targets so they are aware of, can prepare for, and hopefully ward off a potential attack.[28]

41. IBM itself noted in January 2023 in its blog run by IBM Security that the use of third parties can even further increase the risk of an attack for a healthcare provider.[29]

42. Due to the high-profile nature of these breaches and other breaches of its kind, J&J and IBM were on notice and aware of or should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

43. And yet, despite the prevalence of public announcements of data breaches and data security compromises, J&J and IBM failed to take appropriate steps to protect Mr. Jenkins and Class Members' PHI and PII from being compromised.

IV. Hackers Targeted and Gained Access to the CarePath Database in August 2023

44. Sometime on or before September 15, 2023, J&J became aware of a technical method by which unauthorized access to the third-party database managed by IBM for CarePath could be obtained.

45. Upon realizing this, J&J notified IBM and, working with its unnamed third-party database provider, IBM claims to have remediated the issue.

46. IBM also undertook an investigation to assess if there had been access to the database. Through this investigation, it discovered that on August 2, 2023, there was unauthorized access to personal information in the database. IBM stated its investigation was unable to determine the scope of that access.

[28] https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a (last accessed November 21, 2023).
[29] https://securityintelligence.com/news/third-party-risk-healthcare-data-breaches/ last accessed November 21, 2023).

47. The database included personal information about individuals who used CarePath, including contact information, medications, and medical conditions.

48. J&J and IBM were in possession of Mr. Jenkins's PHI and PII and as a result, his information was among the data accessed by an unauthorized third party in the August 2, 2023, data breach.

49. IBM sent Mr. Jenkins a letter dated September 15, 2023, over a month following the breach, informing him of the incident. Until he received this letter, Mr. Jenkins was unaware of the August 2, 2023, data breach.

50. Because IBM failed to send the notice until at least September 15, 2023, an unauthorized actor had access to Mr. Jenkins's PHI and PII for more than a month without Mr. Jenkins's knowledge. It is unclear how long the unauthorized actor has access to Mr. Jenkins's PHI and PII before Defendants discovered the breach and secured Mr. Jenkins' his account and information.

51. IBM's notice only supplied the most basic details about the data breach and did not even disclose the date on which the breach was discovered or when the accounts were secured. It also lacked sufficient information about how the breach occurred, what safeguards Defendants have implemented since then to safeguard against further attacks, and where the information hacked exists today.

52. IBM only offered affected individuals one year of complimentary credit and identity monitoring in its notice. J&J has made no offer of support to affected individuals like Mr. Jenkins beyond what IBM provided.

53. IBM has since disclosed through the U.S. Department of Health and Human Services' Office of Civil Rights' Breach Portal that at least 630,755 individuals were affected by the August 2, 2023, breach.[30]

V. The Effects of the Data Breach

54. J&J and IBM received highly sensitive PHI and PII from Mr. Jenkins in connection with the services Mr. Jenkins received from J&J and IBM through CarePath. As a result, Mr. Jenkins's information was among the data an unauthorized third party accessed in the data breach.

55. Mr. Jenkins was and is very careful about sharing his PHI and PII. He has never knowingly transmitted unencrypted sensitive PHI or PII over the internet or any other unsecured source.

56. Mr. Jenkins stored any documents containing his PHI and PII in a safe and secure location or destroyed the documents. Moreover, he diligently chose unique usernames and passwords for his online accounts.

57. Mr. Jenkins took reasonable steps to maintain the confidentiality of his PHI and PII and relied on J&J and IBM to keep his PHI and PII confidential and securely maintained, and to make only authorized disclosures of this information.

58. The September 15, 2023, Notice from IBM notified Mr. Jenkins that IBM's network had been accessed and that his PHI and PII may have been involved in the data breach.

59. Furthermore, IBM's Notice directed Mr. Jenkins to be vigilant and to take steps to protect his PHI and PII and otherwise mitigate his damages, such as by regularly reviewing his account statements and explanations of benefits from his health insurer or care providers for

[30] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed November 21, 2023).

unauthorized activity. It further provided him with additional resources at his disposal such as contacting nationwide credit reporting agencies and reviewing governmental websites for information about protecting against identity theft.

60. As a result of the data breach, Mr. Jenkins heeded IBM's warnings and spent time dealing with the consequences of the data breach, which included time spent verifying the legitimacy of the Notice and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

61. Mr. Jenkins suffered actual injury in the form of damages to and diminution in the value of his PHI and PII —a form of intangible property that Mr. Jenkins entrusted to J&J and IBM, which was compromised in and because of the data breach.

62. Mr. Jenkins has suffered lost time, annoyance, interference, and inconvenience because of the data breach. He has also suffered from anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PHI and PII.

63. Mr. Jenkins suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PHI and PII being placed in the hands of unauthorized third parties/criminals.

64. Mr. Jenkins has a continuing interest in ensuring that his PHI and PII, which, upon information and belief, remains in J&J and IBM's possession, is protected and safeguarded from future breaches.

VI. J&J and IBM's HIPAA Responsibilities

65. J&J and IBM acquired, collected, stored, and assured reasonable security over Mr. Jenkins and Class Members' PHI and PII.

66. As a condition of their relationships with Mr. Jenkins and Class Members, J&J and IBM required that Mr. Jenkins and Class Members entrust J&J and IBM with highly sensitive and confidential PHI and PII. J&J and IBM, in turn, stored that information on their systems that were ultimately affected by the data breach.

67. By obtaining, collecting, and storing Mr. Jenkins and Class Members' PHI and PII, J&J and IBM assumed legal and equitable duties over the PHI and PII and knew or should have known that they were thereafter responsible for protecting Mr. Jenkins and Class Members' PHI and PII from unauthorized disclosure.

68. Mr. Jenkins and Class Members have taken reasonable steps to maintain their PHI and PII's confidentiality. Mr. Jenkins and Class Members relied on J&J and IBM to keep their PHI and PII confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

69. J&J and IBM could have prevented the data breach, which began as early as August 2, 2023, by properly securing and encrypting and/or more securely encrypting their servers and databases, generally, as well as Mr. Jenkins and Class Members' PHI and PII. J&J and IBM could have prevented the data breach by implementing or more successfully implementing other data security measures including, but not limited to, access controls, employee education, and network monitoring and controls.

70. J&J and IBM's negligence in safeguarding Mr. Jenkins and Class Members' PHI and PII is exacerbated by the increase of the frequency and impact of data breach attacks in recent years which should have served as warnings to J&J and IBM to adequately protect the PHI and PII in their possession.

71. J&J and IBM had and continue to have obligations under HIPAA, applicable federal and state law, reasonable industry standards, common law, and their own assurances and representations to keep Mr. Jenkins and Class Members' PHI and PII confidential and to protect such PHI and PII from unauthorized access.

72. J&J and IBM collected and stored Mr. Jenkins and Class Members' PHI and PII with the reasonable expectation and mutual understanding that J&J and IBM would comply with their obligations to keep such information confidential and secure from unauthorized access.

73. Despite this, even today, Mr. Jenkins and Class Members remain in the dark regarding what data was accessed, the particular mechanism used to access the data, and what steps are being taken to secure their PHI and PII in the future. Thus, Mr. Jenkins and Class Members are left to speculate as to where their PHI and PII ended up, who has used it, and for what nefarious purposes. Indeed, they are left to further speculate as to the full impact of the data breach and how J&J and IBM intend to enhance their information security systems and monitoring capabilities to prevent further breaches.

74. In failing to adequately secure Mr. Jenkins and Class Members' sensitive data, J&J and IBM breached duties they owed Mr. Jenkins and Class Members under statutory and common law. Under HIPAA, health insurance providers and business associates have an affirmative duty to keep patients' protected health information private. As a covered entity, J&J and IBM have a statutory duty under HIPAA and other federal and state statutes to safeguard Mr. Jenkins and Class Members' data. Moreover, Mr. Jenkins and Class Members surrendered their highly sensitive personal data to J&J and IBM under the implied condition that J&J and IBM would keep it private and secure. Accordingly, J&J and IBM also had an implied duty to safeguard their data, independent of any statute.

75. Because J&J and IBM are covered by HIPAA, they are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

76. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for protecting health information.

77. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

78. HIPAA requires J&J and IBM to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

79. "Electronic protected health information" is "individually identifiable health information [...] that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

80. HIPAA's Security Rule requires J&J and IBM to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

81. HIPAA also requires J&J and IBM to "review and modify the security measures implemented [...] as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

82. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires J&J and IBM to provide notice of the data breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

83. J&J and IBM were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

84. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as J&J and IBM, should employ to protect against the unlawful exposure of PHI/PII.

85. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that companies should:

e. Protect the sensitive consumer information that they keep;

f. Properly dispose of PHI and PII that is no longer needed;

g. Encrypt information stored on computer networks;

h. Understand their network's vulnerabilities; and

i. Implement policies to correct security problems.

86. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

87. The FTC recommends that companies not maintain information longer than is necessary for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network and verify that third-party service providers have implemented reasonable security measures.

88. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

89. J&J and IBM's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PHI and PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

90. In addition to their obligations under federal and state laws, J&J and IBM owed a duty to Mr. Jenkins and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI and PII in J&J and IBM's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. J&J and IBM owed a duty to Mr. Jenkins and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected Mr. Jenkins and Class Members' PHI and PII.

91. J&J and IBM owed a duty to Mr. Jenkins and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that all PHI and PII in their possession was adequately secured and protected.

92. J&J and IBM owed a duty to Mr. Jenkins and Class Members to create and implement reasonable data security practices and procedures to protect all PHI and PII in their possession, including not sharing information with other entities who maintain substandard data security systems.

93. J&J and IBM owed a duty to Mr. Jenkins and Class Members to implement processes that would immediately detect a breach of their data security systems in a timely manner.

94. J&J and IBM owed a duty to Mr. Jenkins and Class Members to act upon data security warnings and alerts in a timely fashion.

95. J&J and IBM owed a duty to Mr. Jenkins and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PHI and PII from unauthorized access and theft, because such an inadequacy would be a material fact in the decision to entrust this PHI and PII to J&J and IBM.

96. J&J and IBM owed a duty of care to Mr. Jenkins and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

97. J&J and IBM owed a duty to Mr. Jenkins and Class Members to encrypt and/or more reliably encrypt Mr. Jenkins and Class Members' PHI and PII and monitor it to identify possible threats.

VII. Plaintiff Jenkins Faces a Substantial Risk of Future Injury Because His PHI and PII Were Exposed in the Data Breach

98. Health records and other PHI and PII are a valuable commodity that are a frequent, intentional target of cybercriminals.[31] Companies that collect such information, including J&J and IBM, are well aware of the risk of being targeted by cybercriminals.[32]

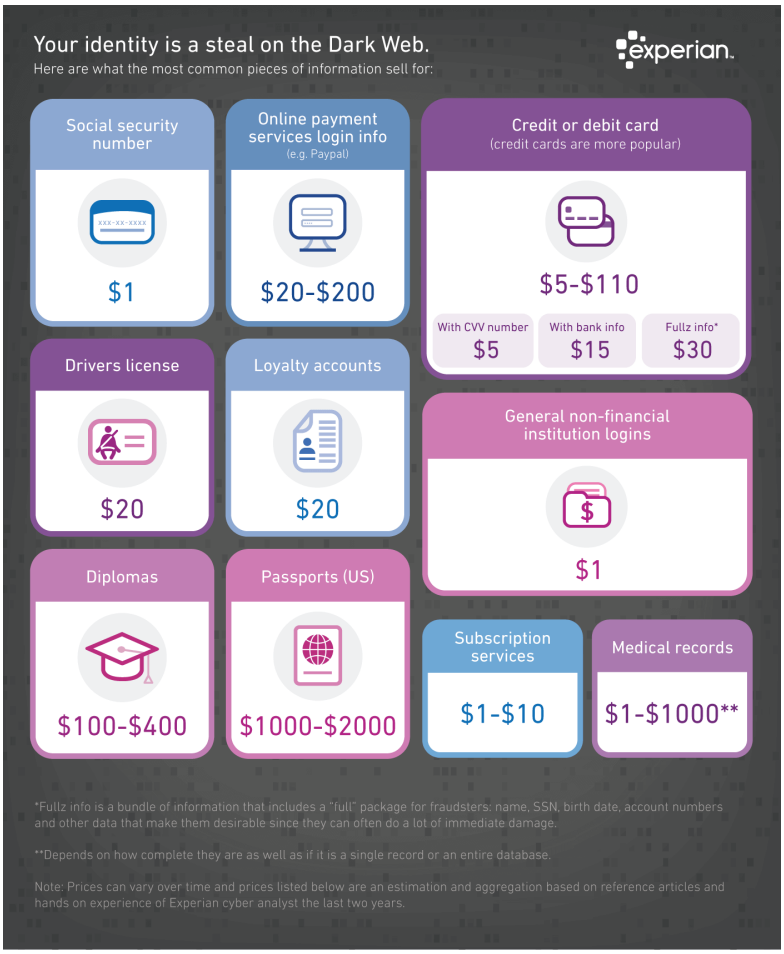
99. Individuals place a high value on their PHI and PII and the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight the impact of identity theft.

100. While the greater efficiency of electronic health records and online resources to provide medication information, like CarePath, translates to cost savings for providers and patients, these also come with the risk of privacy breaches. These electronic records contain sensitive information (e.g., patient data, patient diagnosis, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for up to a thousand dollars on the dark web.[33] PHI and PII are valuable commodities for which a marketplace exists on the dark web where criminals can openly post this personal information for

[31] *See* https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety (last accessed November 21, 2023).
[32] *See, e.g.,* https://www.ibm.com/downloads/cas/DB4GL8YM (last accessed November 21, 2023); J&J 2022 Annual Report ("The extensive information security and cybersecurity threats, which affect companies globally, pose a risk to the security and availability of these systems and networks, and the confidentiality, integrity, and availability of the Company's sensitive data").
[33] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 21, 2023).

sale. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the data breach here.

101. The high value of PHI and PII to criminals is evidenced by the prices they will pay for it through the dark web. In 2017, Experian reported that a stolen credit or debit card number could sell for $5 to $110 on the dark web.[34] In contrast, it reported that medical records could sell for as much as $1000, depending upon the completeness of the record.[35]



[34] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 21, 2023).
[35] *Id.*

102. Since October 2009, there have been over 5,660 healthcare data breaches.[36] From just 2010 to 2022, these breaches exposed 385 million patient records.[37] In fact, this year from just January 1 to June 26, more than 39 million individuals were impacted in healthcare data breaches.[38] In short, data breaches are increasingly common among healthcare systems.

103. These criminal activities have and will result in devastating financial and personal losses to Mr. Jenkins and Class Members. Stolen health data can be used in various ways, but particularly damaging are when criminals use the details of a specific disease or terminal illness to extort a financial payoff from the individual whose information was stolen or use the information for long-term identity theft.[39]

104. An example of the former occurred in 2020, when the theft of patient from a Finnish psychotherapy practice led to hackers demanding ransom, not just from the healthcare provider, but from the patients themselves.[40] The hackers threatened to expose patients' mental health records and even posted at least 300 of these stolen records online when the patients failed to pay the ransom.[41]

105. For patients prescribed other medications supported by CarePath, such as those to manage HIV, the risk of extortion is especially prevalent as two-thirds of US states criminalize

[36] https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last updated November 21, 2023).
[37] https://www.healthcaredive.com/news/tracking-healthcare-data-breaches-cybersecurity-hacking-hospitals/696184/ (last accessed November 21, 2023).
[38] https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far (last accessed November 21, 2023).
[39] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last accessed November 21, 2023).
[40] https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it (last accessed November 21, 2023).
[41] *Id.*; https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/ (last accessed November 21, 2023).

otherwise legal conduct or increase penalties for illegal conduct based upon a person's HIV-positive status.[42]

106. Long-term identity theft is also a substantial risk for individuals who have had their medical information stolen. CBS News reported in 2019 that an individual who had his medical information stolen in 2004 dealt with the ramifications of it for a decade.[43] The hackers used his information to have multiple medical procedures done, ultimately totaling nearly $20,000.[44]

107. Such risks will be omnipresent threats for Plaintiff Jenkins and Class Members for the rest of their lives. They will need to remain constantly vigilant.

108. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

109. Identity thieves can use PHI and PII, such as that of Mr. Jenkins and Class Members which J&J and IBM failed to keep secure, to perpetrate various crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but

[42] https://williamsinstitute.law.ucla.edu/issues/hiv-(last accessed November 21, 2023). criminalization/#:~:text=HIV%20criminalization%20is%20a%20term,a%20person%27s%20HIV%2Dpositive%20status (last accessed November 21, 2023).
[43] https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/ (last accessed November 21, 2023).
[44] *Id.*

with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

110. The ramifications of J&J and IBM's failure to secure Mr. Jenkins and Class Members' PHI and PII are long-lasting and severe. Once PHI and PII is stolen fraudulent use of that information and damage to victims may continue for years. Indeed, Mr. Jenkins and Class Members' PHI and PII was likely taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PHI and PII for that purpose. The fraudulent activity resulting from the data breach may not come to light for years.

111. Individuals, like Mr. Jenkins and Class Members, are particularly concerned with protecting the privacy of their personal information, medical records, and diagnoses.

112. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI and PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[45]

113. The harm to Mr. Jenkins and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most expensive forms of identity theft.[46]

114. When cybercriminals access health insurance information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which J&J and IBM may have exposed Mr. Jenkins and Class Members.

---

[45] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf (last accessed November 21, 2023).
[46] https://www.ibm.com/downloads/cas/3R8N1DZJ (last accessed November 21, 2023).

115. A 2010 study by Ponemon Institute, which was sponsored by Experian, found that the average cost of medical identity theft is about $20,000 per incident, with more than half the victims stating that they were forced to pay for healthcare they did not receive to restore coverage.[47] The study also found that almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one- third of medical identity theft victims saw their insurance premiums rise.[48]

116. A 2018 report by the Internet Society's Online Trust Alliance found that 95% of data breaches are preventable.[49] However, preventing these data breaches requires forethought and planning of the kind IBM sells to other organizations.[50]

117. Here, J&J and IBM knew of the importance of safeguarding PHI and PII and of the foreseeable consequences that would occur if Mr. Jenkins and Class Members' PHI and PII was stolen, including the significant costs that would be placed on Mr. Jenkins and Class Members because of a breach of this magnitude. As detailed above, J&J and IBM knew or should have known that the development and use of such protocols was necessary to fulfill their statutory and common law duties to Mr. Jenkins and Class Members. Therefore, their failure to do so is intentional, willful, reckless, and/or grossly negligent.

118. Furthermore, IBM has offered only a limited one-year subscription for identity theft monitoring and identity theft protection through Equifax. This limitation is inadequate when the victims will likely face many years of identity theft.

---

[47] https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last accessed November 21, 2023).
[48] *Id.*
[49] https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf (last accessed November 21, 2023).
[50] *See, e.g.,* https://www.ibm.com/data-security (last accessed November 21, 2023).

119. Moreover, IBM's credit monitoring offer and advice to Mr. Jenkins and Class Members squarely places the burden on Mr. Jenkins and Class Members, rather than on J&J and IBM, to monitor and report suspicious activities to law enforcement. In other words, IBM expects Mr. Jenkins and Class Members to protect themselves from IBM's tortious acts resulting from the data breach. Rather than automatically enrolling Mr. Jenkins and Class Members in credit monitoring services upon discovery of the data breach, J&J and IBM merely sent instructions to Mr. Jenkins and Class Members about actions they could affirmatively take to protect themselves.

120. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Mr. Jenkins and Class Members' PHI and PII. J&J and IBM disregarded the rights of Mr. Jenkins and Class Members by, inter alia: (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequate security protocols and training practices in place to safeguard Mr. Jenkins and Class Members' PHI and PII, (iii) failing to take standard and reasonably available steps to prevent the data breach, (iv) concealing the existence and extent of the data breach for an unreasonable duration of time, and (v) failing to provide Mr. Jenkins and Class Members prompt and accurate notice of the data breach.

CLASS ACTION ALLEGATIONS

121. Each class's claims derive directly from a course of conduct by J&J and IBM.

122. J&J and IBM have engaged in uniform and standardized conduct toward each class. J&J and IBM did not materially differentiate in their actions or inactions toward members of the respective classes. For each class, the objective facts on these subjects are the same for all class members.

123. Within each Claim for Relief asserted by each class, the same legal standards govern. Accordingly, Plaintiff Jenkins brings this lawsuit as a class action on his own behalf and on behalf of all other persons similarly situated as members of the proposed classes pursuant to Fed. R. Civ. P. 23.

124. Additionally, many states, and for some claims all states, share the same legal standards and elements of proof, allowing for a multistate or nationwide class or classes for some or all claims.

125. This action may be brought and properly maintained as a class action because the questions it presents are of a common or general interest, and of many persons, and also because the parties are numerous, and it is impracticable to bring them all before the court. Plaintiff Jenkins may sue for the benefit of all as a representative party pursuant to Federal Rule of Civil Procedure 23.

The Nationwide Class

126. Plaintiff Jenkins brings this action and seeks to certify and maintain it as a class action under Rules 23(a); (b)(2); and/or (b)(3); and/or (c)(4) of the Federal Rules of Civil Procedure on behalf of himself and a Nationwide Class defined as follows:

> All individuals within the United States of America whose PHI and PII was exposed to unauthorized third parties as a result of the CarePath data breach.

127. Excluded from the Nationwide Class are J&J and IBM, their employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or

affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

The Florida Class

128. In the alternative, Plaintiff Jenkins brings this action and seeks to certify and maintain it as a class action under Rules 23(a); (b)(2); and/or (b)(3); and/or (c)(4) of the Federal Rules of Civil Procedure on behalf of himself and a Florida Class as defined as follows:

> All individuals within the State of Florida a whose PHI and PII was exposed to unauthorized third parties as a result of the CarePath data breach.

129. Excluded from the Florida Class are J&J and IBM, their employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

Numerosity

130. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(1).

131. The members of the classes are so numerous that a joinder of all members would be impracticable. Indeed, there are over 1.16 million patients who used the CarePath website.

132. Those same users had their data compromised as result of J&J and IBM's dangerous data practices.

133. These dangerous data practices put in peril massive amounts of sensitive and protected information about these customers.

134. J&J and IBM have already provided precise numbers associated with data breach in its disclosures to the U.S. Government.

135. The identified number is in the hundreds of thousands and well beyond what is required for the numerosity requirement of Rule 23.

Ascertainability

136. The classes are ascertainable.

137. The defined classes consist of only those individuals whose PHI and PII was exposed to unauthorized third parties as a result of the CarePath data breach. The very data that J&J and IBM have put in peril makes them capable of identifying these individuals precisely.

138. Indeed, the data that was compromised includes identifying information which can be used to provide members of each class with direct notice pursuant to the requirements of Rule 23 and the Due Process Clause of the United States Constitution.

139. In addition, because the data available about members of the classes is so granular, other forms of notice can be effectively used, including notice through e-mail or other electronic means; through broadcast media; through publication, including in newspapers; and through direct mailing.

140. J&J and IBM have demonstrated that they are capable of directly contacting members of the classes that are affected by their data breach, as they have (a) directly sent letters to these individuals, and (b) provided notice to them through postings on J&J and IBM's websites.

141. J&J and IBM would be hard pressed to contest the ascertainability of the classes, as it used the above means to communicate with class members directly.

Typicality

142. Plaintiff Jenkins's claims are typical of the members of the classes.

143. Plaintiff Jenkins's claims are the same as those asserted by members of the classes. Plaintiff Jenkins, like the members of the classes, faces a substantial risk of harm as a

result of J&J and IBM's practices which led to the CarePath data breach, and has been harmed by those practices in a manner typical of each of the classes.

144. Plaintiff Jenkins alleges injury that is not unique to him but is typical of members of each of the classes, including measures of damages, such as benefit of the bargain damages, out-of-pocket losses, and/or nominal damages.

145. Plaintiff Jenkins alleges that his injury flows from the common course of conduct alleged as to J&J and IBM's conduct, including J&J and IBM's reckless data practices.

146. Plaintiff Jenkins is similarly positioned as to each member of the classes. As such, his injury can be redressed in the same manner as any redress provided to the members of the classes (and vice versa).

Adequate Representation

147. Plaintiff Jenkins will fairly and adequately protect the interests of the class members.

148. Plaintiff Jenkins is committed to putting the interest of the classes ahead of his own and to act in the best interest of members of the classes.

149. Plaintiff Jenkins understands his obligations to the classes and is committed to monitoring and supervising developments in the case and class counsel.

150. Plaintiff Jenkins has retained competent counsel experienced in computer science, machine- learning, artificial intelligence, data science, cloud-based computer systems, databases, computer security, and encryption.

151. Plaintiff Jenkins has retained counsel with the resources and capital to litigate the case on behalf of the classes.

152. Plaintiff Jenkins and his counsel intend to prosecute this action vigorously and to obtain relief, including both injunctive and monetary relief, that will remedy the root problem at J&J and IBM rather than merely treat the symptoms (i.e., address only a particular data breach without addressing J&J and IBM's reckless data practices).

Superiority

153. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because J&J and IBM have acted and/or refused to act on grounds generally applicable to the classes, thereby making final injunctive and/or corresponding declaratory relief appropriate with respect to each class as a whole.

154. The class device is superior to all other available methods of adjudication, as it would make little sense for each of hundreds of thousands of current, former, and prospective CarePath users to separately prove the common conduct in which J&J and IBM have engaged.

155. Moreover, damages suffered by each individual member of the classes may be small, meaning that the expense or burden of individual litigation would make it very difficult or impossible for individual class members to redress their injury individually.

156. Because damages may be small, individual members of the classes may not have a rational economic interest in individually controlling the prosecution of a single action, and the burden imposed on the judicial system from having to individually adjudicate such claims will be significant in comparison to the value of individual claims.

157. Class litigation is thus superior to individual litigation and is the best procedural device to vindicate the rights of the members of the classes.

158. In addition, class litigation will streamline the management of the litigation, such that the expense, burdens, inconsistencies, economic infeasibility, and other negative effects of individual mitigation will be lessened if not eliminated.

159. The classes expressly disclaim any recovery in this action for physical injury resulting from the centralization of database and system credentials and the centralization and aggregation of current, former, and prospective customer data by J&J and IBM.

160. In sum, class litigation is superior because it mitigates significant inefficiencies and barriers that would result from individual litigation. In fact, absent invocation of the class device, the classes' claims would likely not be vindicated individually, and J&J and IBM's pernicious data and credential centralization practices will persist.

Commonality and Predominance

161. This action and the claims asserted by the classes satisfy the requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) because there are many questions of law and fact that are common as to all of the members of the classes.

162. These questions of fact and law concern J&J and IBM's conduct, which is common as to the members of the classes, and answers to those questions would provide answers to issues posed by claims asserted by all members of the classes.

163. These common issues will predominate at trial, and any individual issues that may arise would not outweigh the predominance of common issues.

164. Common issues that will predominate at trial include, without limitation, the following:

a. Whether Defendants had a legal duty to Plaintiff Jenkins and the Classes to exercise due care in collecting, storing, using, and/or safeguarding their PHI and PII;

b. Whether Defendants knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendants' failure to implement adequate data security measures allowed the data breach to occur;

e. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff Jenkins and Class Members that their PHI and PII had been compromised;

g. How and when Defendants actually learned of the data breach;

h. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the unauthorized access of Plaintiff Jenkins and Class Members' PHI and PII;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff Jenkins and Class Members' PHI and PII;

k. Whether Plaintiff Jenkins and Class Members are entitled to actual and/or statutory damages and/or injunctive, corrective, and/or declaratory relief;

l. Whether an accounting is appropriate as a result of Defendants' wrongful conduct;

m. Whether Plaintiff Jenkins and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

Grounds Generally Applicable to the Classes

165. Plaintiff Jenkins intends to seek injunctive relief ending J&J and IBM's dangerous data practices which caused the CarePath data breach, exposing sweeping amounts of customer (and potentially prospective / former customer) data.

166. Plaintiff Jenkins is properly situated to seek such an injunction because J&J and IBM have acted and/or refused to act on grounds generally applicable to Plaintiff Jenkins and the members of the classes.

167. This means that final injunctive relief or declaratory relief will redress Plaintiff Jenkins's harm as well as the members of the classes.

168. For example, an injunction preventing J&J and IBM from continuing to recklessly manage data, will address a significant risk that imperils the data belonging to Plaintiff Jenkins and the members of the classes.

REALLEGATION AND INCORPORATION BY REFERENCE

169. Plaintiff Jenkins realleges and incorporates by reference all the preceding paragraphs and allegations of this Complaint, as though fully set forth in each of the following Claims for Relief asserted on behalf of the classes.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On behalf of the Nationwide Class, or in the alternative, the Florida Class)

170. At all times herein relevant, Defendants J&J and IBM owed Plaintiff Jenkins and the Nationwide Class, or in the alternative the Florida Class, ("Class Members") a duty of care, inter alia, to act with reasonable care to secure and safeguard their PHI and PII and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing Plaintiff Jenkins and Class Members' PHI and PII on their computer systems and networks.

171. Among these duties, Defendants were expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI and PII in their possession;

b. to protect Plaintiff Jenkins and Class Members' PHI and PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect data breaches quickly and to act on warnings about data breaches in a timely manner; and

d. to promptly notify Plaintiff Jenkins and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PHI and PII.

172. Defendants knew or should have known that Plaintiff Jenkins and Class Members' PHI and PII was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care to not subject Plaintiff Jenkins and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

173. Defendants knew or should have known of the risks inherent in collecting and storing PHI and PII, the vulnerabilities of their data security systems, and the importance of adequate security. Defendants knew or should have known about the numerous well-publicized data breaches of healthcare data systems in recent years.

174. Defendants knew or should have known that their data systems and networks did not adequately safeguard Plaintiff Jenkins and Class Members' PHI and PII.

175. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PHI and PII that Plaintiff Jenkins and Class Members had entrusted to them.

176. Defendants breached their duties to Plaintiff Jenkins and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PHI and PII.

177. Because Defendants knew that a breach of their systems could damage numerous individuals, including Plaintiff Jenkins and Class Members, Defendants had a duty to adequately protect their data systems and the PHI and PII they stored on those systems.

178. Plaintiff Jenkins and Class Members' willingness to entrust Defendants with their PHI and PII was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants could protect their systems and the PHI and PII they stored on them from attack. Thus, Defendants had a special relationship with Plaintiff Jenkins and Class Members.

179. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiff Jenkins and Class Members' PHI and PII and

promptly notify them about the data breach. These independent duties are untethered to any contract between Defendants, Plaintiff Jenkins, and Class Members.

180. Defendants breached their general duty of care to Plaintiff Jenkins and Class Members in, but not limited to, the following ways:

a. by failing to provide fair, reasonable, and/or adequate computer systems and data security practices to safeguard Plaintiff Jenkins and Class Members' PHI and PII;

b. by failing to timely and accurately disclose that Plaintiff Jenkins and Class Members' PHI and PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard PHI and PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI and PII;

d. by failing to provide adequate supervision and oversight of the PHI and PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Plaintiff Jenkins and Class Members' PHI and PII, misuse the PHI and PII, and intentionally disclose it to others without consent;

e. by failing to adequately train their employees and/or their third-party service providers on data security practices;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff Jenkins and Class Members' PHI and PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt or adequately protect Plaintiff Jenkins and Class Members' PHI and PII and monitor their systems in order to identify possible threats.

181. In addition to Defendants' general duty of care, Defendants also had legal duties to protect Plaintiff Jenkins and Class Members' PHI and PII beyond any contractual duties as alleged herein.

182. Defendants' willful failure to abide by these duties was wrongful, reckless, and/or grossly negligent in light of the foreseeable risks and known threats.

183. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Plaintiff Jenkins and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

184. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PHI and PII to Plaintiff Jenkins and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PHI and PII.

185. Defendants breached their duty to notify Plaintiff Jenkins and Class Members of the unauthorized access by waiting roughly two months after learning of the data breach to notify Plaintiff Jenkins and Class Members and then by failing and continuing to fail to provide Plaintiff Jenkins and Class Members sufficient information regarding the breach. To date, Defendants have not provided sufficient information to Plaintiff Jenkins and Class Members regarding the extent of the unauthorized access and other important details, and in failing to do so, continues to breach their disclosure obligations to Plaintiff Jenkins and Class Members.

186. Further, explicitly failing to provide timely and clear notification of the data breach to Plaintiff Jenkins and Class Members, Defendants prevented Plaintiff Jenkins and Class Members from taking meaningful, proactive steps to secure their PHI and PII.

187. There is a close causal connection between Defendants' failure to implement security measures to protect Plaintiff Jenkins and Class Members' PHI and PII and the harm (or risk of imminent harm suffered) by Plaintiff Jenkins and Class Members. Plaintiff Jenkins and Class Members' PHI and PII was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PHI and PII by adopting, implementing, and maintaining appropriate security measures.

188. Defendants' wrongful actions, inactions, and omissions constitute common law negligence.

189. The damages Plaintiff Jenkins and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

190. Additionally, Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair [. . .] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PHI and PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

191. Defendants violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI and PII and by not complying with applicable industry standards, as described in detail herein.

192. Defendants' conduct was particularly unreasonable given the nature and amount of PHI and PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff Jenkins and Class Members.

193. Defendants' violation of 15 U.S.C. § 45 constitutes negligence *per se*. Defendants also violated the HIPAA Privacy and Security Rules, which constitutes negligence *per se*.

194. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff Jenkins and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PHI and PII is used, (iii) the compromise, publication, and/or theft of their PHI and PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI and PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) lost continuity in relation to their healthcare, (vii) the continued risk to their PHI and PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff Jenkins and Class Members' PHI and PII in their continued possession, and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI and PII compromised as a result of the data breach for the remainder of the lives of Plaintiff Jenkins and Class Members.

195. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff Jenkins and Class Members have suffered and will continue to suffer other forms of

injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

196. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff Jenkins and Class Members have suffered and will continue to suffer the continued risks of exposure of their PHI and PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PHI and PII in their continued possession.

COUNT II
Negligence *Per Se*
(On behalf of the Nationwide Class, or in the alternative, the Florida Class)

197. HIPAA requires that covered entities and business associates "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" and "must reasonably safeguard protected health information from any intentional or unintentional use or disclosure . . ." 45 CFR § 164.530I.

198. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 requires HIPAA covered entities and their business associates to provide notification to the United States Department of Health and Human Services, prominent media outlets following a data breach or any breach of unsecured protected health information without unreasonable delay and in no event later than 60 days after discovery of a data breach.

199. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits companies such as Defendants from "using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce," including failing to use reasonable measures to protect PHI and PII. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers'

privacy and security. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

200. In addition to the FTC rules and regulations and state law, other states and jurisdictions where victims of the data breach are located require that Defendants protect PHI and PII from unauthorized access and disclosure and timely notify the victim of a data breach.

201. For example, Florida Statute § 501.171 requires all covered entities and third-party agent to "take reasonable measures to protect and secure data in electronic form containing personal information" and to notify Florida residents affected by a security breach of "as expeditiously as practicable and without unreasonable delay."

202. Defendants violated HIPAA and FTC rules and regulations obligating companies to use reasonable measures to protect PHI and PII by failing to comply with applicable industry standards and by unduly delaying reasonable notice of the actual breach. Defendants' conduct was particularly unreasonable given the nature and amount of PHI and PII it obtained and stored and the foreseeable consequences of a data breach and the exposure of Plaintiff Jenkins and Class Members' highly sensitive PHI and PII.

203. Each of Defendants' statutory violations of HIPAA, Section 5 of the FTC Act and other applicable statutes, rules and regulations, constitutes negligence *per se*.

204. Plaintiff Jenkins and Class Members are within the category of persons HIPAA and the FTC Act were intended to protect.

205. The harm that occurred because of the data breach described herein is the type of harm HIPAA and the FTC Act were intended to guard against.

206. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff Jenkins and Class Members have been damaged as described herein, continue to suffer injuries

as detailed above, are subject to the continued risk of exposure of their PHI and PII in Defendants' possession and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Confidence
(On behalf of the Nationwide Class)

207. During Plaintiff Jenkins and Class Members' interactions with Defendants, Defendants were fully aware of the confidential nature of the PHI and PII that Plaintiff Jenkins and Class Members provided to them.

208. As alleged herein and above, Defendants' relationship with Plaintiff Jenkins and Class Members was governed by promises and expectations that Plaintiff Jenkins and Class Members' PHI and PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

209. Plaintiff Jenkins and Class Members provided their respective PHI and PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PHI and PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

210. Plaintiff Jenkins and Class Members also provided their PHI and PII to Defendants with the explicit and implicit understanding that Defendants would take precautions to protect their PHI and PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems.

211. Defendants voluntarily received, in confidence, Plaintiff Jenkins and Class Members' PHI and PII with the understanding that the PHI and PII would not be accessed by,

acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

212. Defendants voluntarily assumed the duty to maintain the confidentiality of Plaintiff Jenkins and Class Members' PHI and PII and prevent it from being accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

213. Defendants intentionally, knowingly, or negligently failed to maintain the confidentiality of Plaintiff Jenkins and Class Members' PHI and PII by failing to prevent, detect and avoid the data breach from occurring by, inter alia, not following best information security practices to secure Plaintiff Jenkins and Class Members' PHI and PII.

214. Due to Defendants' failure to prevent, detect, and avoid the data breach from occurring by not following best information security practices to secure Plaintiff Jenkins and Class Members' PHI and PII, Plaintiff Jenkins and Class Members' PHI and PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiff Jenkins and Class Members' confidence and without their express permission.

215. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff Jenkins and Class Members have suffered damages, as alleged herein.

216. But for Defendants' failure to maintain and protect Plaintiff Jenkins and Class Members' PHI and PII in violation of the parties' understanding of confidence, their PHI and PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

Defendants' failure to do so and the resulting data breach were the direct and legal cause of the misuse of Plaintiff Jenkins and Class Members' PHI and PII and the resulting damages.

217. The injury and harm Plaintiff Jenkins and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendants' failure to prevent the unauthorized misuse of Plaintiff Jenkins and Class Members' PHI and PII. Defendants knew their data systems and protocols for accepting and securing Plaintiff Jenkins and Class Members' PHI and PII had security and other vulnerabilities that placed Plaintiff Jenkins and Class Members' PHI and PII in jeopardy.

218. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff Jenkins and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PHI and PII is used, (iii) the compromise, publication, and/or theft of their PHI and PII, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI and PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) the continued risk to their PHI and PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff Jenkins and Class Members' PHI and PII in their continued possession, and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI and PII compromised as a result of the data breach for the remainder of the lives of Plaintiff Jenkins and Class Members.

COUNT IV
Breach of Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class)

219. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

220. Plaintiff Jenkins and Class Members have entered into a contract with J&J in the form of the Terms of Service of the CarePath website and the incorporated Privacy Policy.

221. Plaintiff Jenkins and Class Members have complied with and performed all conditions of their contracts with Defendants.

222. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI and PII, failing to timely and accurately disclose the data breach to Plaintiff Jenkins and Class Members, and continuing to acceptance PHI and PII and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the data breach.

223. Defendants acted in bad faith and/or with malicious motive in denying Plaintiff Jenkins and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT V
Breach of Fiduciary Duty
(On behalf of the Nationwide Class, or in the alternative, the Florida Class)

224. In light of the special relationship between Defendants, Plaintiff Jenkins, and Class Members, whereby Defendants became the guardians of Plaintiff Jenkins and Class Members' PHI and PII, Defendants became fiduciaries by their undertaking and guardianship of

the PHI and PII to act primarily for Plaintiff Jenkins and Class Members, (i) for the safeguarding of Plaintiff Jenkins and Class Members' PHI and PII, (ii) to timely notify Plaintiff Jenkins and Class Members of a data breach and disclosure, and (iii) to maintain complete and accurate records of what information (and where) Defendants did have and continue to store.

225. Defendants have a fiduciary duty to act for the benefit of Plaintiff Jenkins and Class Members upon matters within the scope of their relationship with Plaintiff Jenkins and Class Members—in particular, to keep their PHI and PII secure.

226. Defendants knowingly breached their fiduciary duties to Plaintiff Jenkins and Class Members by failing to diligently discover, investigate, and give notice of the data breach in a reasonable and practicable period of time.

227. Defendants knowingly breached their fiduciary duties to Plaintiff Jenkins and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff Jenkins and Class Members' PHI and PII.

228. Defendants knowingly breached their fiduciary duties to Plaintiff Jenkins and Class Members by failing to timely notify and/or warn Plaintiff Jenkins and Class Members of the data breach.

229. Defendants knowingly breached their fiduciary duties to Plaintiff Jenkins and Class Members by otherwise failing to safeguard Plaintiff Jenkins and Class Members' PHI and PII.

230. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff Jenkins and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PHI and PII is used, (iii) the compromise, publication, and/or theft of their PHI and PII, (iv) out-of-pocket

expenses associated with the prevention, detection and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI and PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) the continued risk to their PHI and PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff Jenkins and Class Members' PHI and PII in their continued possession, and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI and PII compromised as a result of the data breach for the remainder of the lives of Plaintiff Jenkins and Class Members.

231. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff Jenkins and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
Unjust Enrichment
(On behalf of the Nationwide Class, or in the alternative, the Florida Class)

232. Plaintiff Jenkins brings this cause of action on his own behalf and on behalf of the Class Members against Defendants.

233. This cause of action is pleaded in the alternative to the legal claims asserted.

234. Plaintiff Jenkins lacks an adequate remedy at law for his claim, as specifically set forth later in this complaint.

235. J&J received the benefit of obtaining Plaintiff Jenkins and Class Members' PHI and PII regarding their insurance coverage and use of J&J prescription medications.

236. On information and belief, J&J used this PHI and PII to obtain financial benefits.

237. IBM received funds in connection with managing CarePath data, including Plaintiff Jenkins and Class Members' PHI and PII regarding their insurance coverage and use of J&J prescription medications.

238. The PHI and PII were benefits conferred upon Defendants by Plaintiff Jenkins and Class Members.

239. Defendants were unjustly enriched through financial benefits conferred upon them by Plaintiff Jenkins and Class Members.

240. Defendants knew and understood that they would and did receive a financial benefit, and voluntarily accepted the same by obtaining and maintaining Plaintiff Jenkins and Class Members' PHI and PII when they elected to sign up for CarePath.

241. By signing up for and utilizing CarePath, Plaintiff Jenkins and Class Members reasonably expected that Defendants would use fair, reasonable, or adequate computer systems and data security practices to safeguard their PHI and PII. Defendants fell short of such expectations, they injured and damaged Plaintiff Jenkins and Class Members in doing so. Defendants were enriched, while at the same time, Plaintiff Jenkins and Class Members experienced a diminution of value to their PHI and PII.

242. Therefore, because Defendants will be unjustly enriched if they are allowed to retain the revenues obtained through their negligence and unlawful conduct, Plaintiff Jenkins and Class Members are entitled to recover the amount by which Defendants were unjustly enriched at their expense.

243. Accordingly, Plaintiff Jenkins, on behalf of himself and each Class Member, seeks damages against Defendants in the amounts by which Defendants have been unjustly

enriched at Plaintiff Jenkins and Class Members' expense, and such other relief as this Court deems just and proper.

COUNT VII
Violation of Florida Deceptive and Unfair Trade Practices Act
(On behalf of the Florida Class)

244. Defendants engaged in conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendants obtained Plaintiff Jenkins and Florida Class members' PHI and PII through advertising, soliciting; providing; offering, and/or distributing services to Plaintiff Jenkins and the Florida Class Members and the data breach occurred through the use of the internet, an instrumentality of interstate commerce.

245. Defendants engaged in unfair or deceptive acts or practices in the conduct of consumers transactions, including, among other things:

a. failing to implement adequate data security practices to safeguard PHI and PII;

b. failing to make only authorized disclosures of Plaintiff Jenkins and Florida Class Members' PHI and PII;

c. failing to disclose that their data security practices where inadequate to safeguard PHI and PII from theft; and

d. failure to timely, accurately, and completely disclose the data breach to Plaintiff Jenkins and Florida Class Members.

246. Defendants' actions constitute unconscionable, deceptive, or unfair acts or practices because Defendants engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Plaintiff Jenkins and Florida Class Members by failing to adequately protect their PHI and PII.

247. Defendants also engaged unconscionable, deceptive, or unfair acts or practices by omitting, failing to disclose, or inadequately disclosing to Plaintiff Jenkins and Florida Class Members that they did not follow industry best practices for the collection, use, and storage of PHI and PII.

248. As a direct and proximate result of Defendants' conduct, Plaintiff Jenkins and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PHI and PII is used, (iii) the compromise, publication, and/or theft of their PHI and PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI and PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) the continued risk to their PHI and PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff Jenkins and Class Members' PHI and PII in their continued possession, and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI and PII compromised as a result of the data breach for the remainder of the lives of Plaintiff Jenkins and Class Members.

249. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts, Plaintiff Jenkins and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

250. As a direct result of Defendants' knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff Jenkins and Florida Class Members are entitled to injunctive relief, including, but not limited to, an injunction is required to prevent the further unauthorized disclosures of Plaintiff Jenkins and Class Members' PHI and PII.

LACK OF ADEQUATE REMEDIES AT LAW

251. Plaintiff Jenkins lacks an adequate remedy at law for his claims to the extent they seek relief that is equitable in nature.

252. ***Injunctive relief.*** Plaintiff Jenkins seeks injunctive relief to enjoin Defendants from continuing their campaign of unlawful data practices.

253. Defendants continue to maintain and obtain PHI and PII, including Plaintiff Jenkins and Class Members' PHI and PII, which creates a continuing risk to their PHI and PII so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff Jenkins and Class Members' PHI and PII.

254. An injunction is required to prevent the further unauthorized disclosures of Plaintiff Jenkins and Class Members' PHI and PII. Legal remedies, such as damages, cannot prevent such continued harm.

255. In addition, absent an injunction, Plaintiff Jenkins and Class Members can no longer rely on Defendants' statements about their privacy protections and data security practices. Thus, absent an injunction, Plaintiff Jenkins and Class Members will abstain from further use of CarePath.

256. Absent such an option, Plaintiff Jenkins and Class Members cannot obtain complete relief. Such relief is purely equitable in nature and unavailable at law.

257. Indeed, damages available at law would still leave Plaintiff Jenkins and Class Members with a risk of further unauthorized access of their PHI and PII.

258. ***Alternative Pleading.*** Plaintiff Jenkins also pleads his equitable claims in the alternative to his legal claims. Thus, for example, any equitable restitution available under the unjust enrichment claims asserted cannot possibly be asserted alongside legal claims, as Plaintiff Jenkins seeks to press those equitable claims only if he does not prevail on claims providing legal remedies.

259. This alternative pleading is necessary to ensure that Plaintiff Jenkins retains equitable remedies if, for example, claims providing legal remedies are dismissed or judgment is rendered upon them prior to trial.

260. Moreover, if Plaintiff Jenkins prevails at trial on claims providing legal remedies, Plaintiff Jenkins's claims for equitable restitution will necessarily fail (and would not be asserted) to the extent co-extensive with monetary damages obtained at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Jenkins requests that judgment be entered against Defendants and that the Court grant the following:

A. Enter an order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23;

B. Enter a judgment against Defendants in favor of Plaintiff Jenkins and the proposed classes;

C. Award damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

D. Enjoin Defendants and order them to cease and desist for continuing in their unlawful activities;

E. Award equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff Jenkins and Class Members' PHI and PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff Jenkins and Class Members;

F. Issue relief requested by Plaintiff Jenkins and Class Members, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Plaintiff Jenkins and Class Members, including but not limited to an Order:

1. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
2. requiring Defendants to protect all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;
3. requiring Defendants to delete and purge Plaintiff Jenkins and Class Members' PHI and PII unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff Jenkins and Class Members;
4. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff Jenkins and Class Members' PHI and PII;
5. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

6. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;
7. requiring Defendants to conduct regular database scanning and securing checks;
8. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI and PII, as well as protecting the PHI and PII of Plaintiff Jenkins and Class Members;
9. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs and systems for protecting personal identifying information;
10. requiring Defendants to implement, maintain, review and revise as necessary a threat management program to monitor Defendants' networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested and updated;
11. requiring Defendants to meaningfully educate all Class Members about the threats they face as a result of the loss of their confidential PHI and PII to third parties, as well as the steps affected individuals must take to protect themselves.

G. Award prejudgment interest on all amounts awarded, at the prevailing legal rate;

H. Award Plaintiff Jenkins and the proposed classes their costs of suit, including reasonable attorneys' fees as provided by law; and

I. Award such further and additional relief as the case may require and the Court may deem just and proper under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all claims so triable as a matter of right.

Dated: November 21, 2023

Respectfully submitted,

AHDOOT & WOLFSON, PC

Tina Wolfson (NY 5436043)
twolfson@ahdootwolfson.com
Deborah De Villa (NY 5724315)
ddevilla@ahdootwolfson.com
521 Fifth Avenue | 17th Floor
New York, NY 10175
Tel (917) 336-0171
Fax (917) 336-0177

BATHAEE DUNNE LLP

/s/ Andrew Chan Wolinsky
Andrew Chan Wolinsky (NY 4892196)
awolinsky@bathaeedunne.com
Yavar Bathaee (NY 4703443)
yavar@bathaeedunne.com
Chang Hahn (NY 5921911)
chahn@bathaeedunne.com
445 Park Avenue, 9th Floor
New York, NY 10022
Tel.: (332) 322-8835

Brian J. Dunne (NY 4605580)
bdunne@bathaeedunne.com
Edward M. Grauman (NY 4196390)
egrauman@bathaeedunne.com
901 South MoPac Expressway
Barton Oaks Plaza I, Suite 300
Austin, TX 78746
Tel.: (213) 462-2772

Allison Watson Cross (*p.h.v. forthcoming*)
across@bathaeedunne.com
3420 Bristol Street, Suite 600
Costa Mesa, CA 92626
Tel: (213) 462-2772